

EXHIBIT 2

IN THE UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
TAMPA DIVISION

UNITED STATES OF AMERICA

v.

Case No. 8:12-CR-45-T-35AEP

SAMI OSMAKAC

**GOVERNMENT’S UNCLASSIFIED MEMORANDUM IN OPPOSITION
TO SAMI OSMAKAC’S “SUPPLEMENTAL MOTION TO SECOND
MOTION FOR DISCLOSURE OF FISA INTERCEPTIONS AND
ANCILLARY CIPA RESTRICTIONS IN SUPPORT OF EVIDENCE TO
BE PRESENTED (DKT #100) AND MOTION FOR DISCLOSURE OF
FISA INTERCEPTIONS AND ANCILLARY CIPA RESTRICTIONS IN
SUPPORT OF EVIDENCE TO BE PRESENTED (DKT 98) AND
INCORPORATED MEMORANDUM OF LAW”**

I. INTRODUCTION

The Government is filing this unclassified version of its classified memorandum (Memorandum) in opposition to a motion filed on May 2, 2013, by Sami Osmakac (Osmakac or the defendant) entitled “*Supplemental Motion to Second Motion for Disclosure of FISA Interceptions and Ancillary CIPA Restrictions In Support of Evidence to be Presented (Dkt #100) and To Motion for Disclosure of FISA Interceptions and Ancillary CIPA Restrictions in Support of Evidence to be Presented (Dkt 98) and Incorporated Memorandum of Law*” (Defendant’s Motion) (Document 121). Defendant’s Motion specifically requests “this Court to review and disclose the underlying [Foreign Intelligence Surveillance Act (FISA)] applications and orders,” which calls for the disclosure of classified materials filed with the Foreign Intelligence Surveillance Court (FISC) (the FISA materials).¹

CLASSIFIED MATERIAL REDACTED^{2 3 4 5}

The Government expects that the Court will conclude from its *in camera*, *ex parte* review of the FISA materials that: (1) the electronic surveillance and physical

¹ **CLASSIFIED MATERIAL REDACTED**

² As a result of the redactions, the pagination and footnote numbering of the classified memorandum and the unclassified memorandum are different.

³ The provisions of FISA that address electronic surveillance are found at 50 U.S.C. §§ 1801-1812; those that address physical searches are found at 50 U.S.C. §§ 1821-1829. These two sets of provisions are in many respects parallel and almost identical. Citations herein are generally to the two sets of provisions in parallel, with the first citation being to the relevant electronic surveillance provision, and the second citation being to the relevant physical search provision.

⁴ “Aggrieved person” is discussed *infra* at footnote 7.

⁵ The Attorney General’s affidavit (*Declaration and Claim of Privilege*) is being filed both publicly and as part of the classified filing.

searches at issue in this case were both lawfully authorized and lawfully conducted in compliance with the Fourth Amendment; (2) disclosure to the defendant of the FISA materials and the Government's classified submissions is not authorized because the Court is able to make an accurate determination of the legality of the surveillance without disclosing the FISA materials or portions thereof; and (3) the defendant's discovery request should be denied to the extent that it seeks disclosure of the FISA materials. For the reasons set forth below, the Court should deny Defendant's Motion.

A. BACKGROUND

On January 7, 2012, Osmakac was arrested by the Federal Bureau of Investigation (FBI) on a criminal complaint after he took possession of what he believed to be a car bomb and other weapons. On February 2, 2012, Osmakac was indicted by a federal grand jury in the Middle District of Florida on the charges of Attempting to Use a Weapon of Mass Destruction, in violation of 18 U.S.C. § 2332a(a)(2)(A), and Illegally Possessing a Firearm, in violation of 26 U.S.C. § 5861(d). A trial date has been set for October 21, 2013.

CLASSIFIED MATERIAL REDACTED

On February 17, 2012, Osmakac and this Court were provided with notice pursuant to 50 U.S.C. §§ 1806(c) and 1825(d) that the United States "intends to offer into evidence, or otherwise use or disclose in any proceedings in the above-captioned matter, information obtained and derived from electronic surveillance or physical search conducted pursuant to the Foreign Intelligence Surveillance Act of 1978 (FISA), as amended, 50 U.S.C. §§ 1801-1811, 1821-1829." (Document 20).

CLASSIFIED MATERIAL REDACTED

On May 2, 2013, Osmakac filed a motion to, among other things, disclose the FISA applications and orders. (Document 121.)

CLASSIFIED MATERIAL REDACTED

In subsequent sections of this Memorandum, the Government will: (1) present an overview of the FISA authorities at issue in this case; (2) discuss the FISA process; (3) address the manner in which the Court should conduct its *in camera, ex parte* review of the FISA materials; (4) summarize in some detail the facts supporting the FISC's probable cause determinations with respect to the targets of the electronic surveillance and physical searches and to the facilities, places, premises, or property targeted (all of which information is contained fully in the exhibits in the Sealed Appendix); and (5) discuss the relevant minimization procedures. All of the Government's pleadings and supporting FISA materials are being submitted not only to oppose Defendant's Motion, but also to support the United States' request, pursuant to FISA, that this Court: (1) conduct an *in camera, ex parte* review of the FISA materials; (2) find that the FISA information at issue was lawfully acquired and that the electronic surveillance and physical searches were made in conformity with an order of authorization or approval;⁶ and (3) order that none of the FISA materials be disclosed to the defense, and instead, that they be maintained by the United States under seal.

B. OVERVIEW OF THE FISA AUTHORITIES**CLASSIFIED MATERIAL REDACTED**

⁶ Should Osmakac file a motion to suppress FISA-obtained or derived information, the Government submits these same arguments herein would also establish that such information should not be suppressed.

1. The FISA Authorities

a. CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED

b. CLASSIFIED MATERIAL REDACTED

2. The FISC's Findings

CLASSIFIED MATERIAL REDACTED

II. THE FISA PROCESS

A. OVERVIEW OF FISA

Enacted in 1978, and subsequently amended, FISA authorizes the Chief Justice of the United States to designate eleven United States District Judges to sit as judges of the FISC. 50 U.S.C. § 1803(a)(1). The FISC judges are empowered to consider *ex parte* applications submitted by the Executive Branch for electronic surveillance and physical searches when a significant purpose of the application is to obtain foreign intelligence information, as defined in FISA. Rulings of the FISC are subject to review by the Foreign Intelligence Surveillance Court of Review (FISC of Review), which is composed of three United States District or Circuit Judges who are designated by the Chief Justice. 50 U.S.C. § 1803(b). As discussed below, a District Court also has jurisdiction to determine the legality of electronic surveillance and physical searches authorized by the FISC when the fruits of that intelligence collection are used against an “aggrieved person.”⁷ 50 U.S.C. §§ 1806(f), 1825(g).

⁷ An “aggrieved person” is defined as the target of electronic surveillance or “any other person whose communications or activities were subject to electronic surveillance,” 50 U.S.C. § 1801(k), as well as “a person whose premises, property, information, or material is the target of physical search” or “whose premises, property, information, or material was subject to physical search. 50 U.S.C. § 1821(2). The

As originally enacted, FISA required that a high-ranking member of the Executive Branch of Government certify that “the purpose” of the FISA application was to obtain foreign intelligence information. In 2001, FISA was amended as part of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act).⁸ One change to FISA accomplished by the USA PATRIOT Act is that a high-ranking official is now required to certify that the acquisition of foreign intelligence information is “a significant purpose” of the requested surveillance. 18 U.S.C. § 1804(a)(6)(B).

CLASSIFIED MATERIAL REDACTED^{9 10}

B. THE FISA APPLICATION

FISA provides a statutory procedure whereby the Executive Branch may obtain a judicial order authorizing the use of electronic surveillance, physical searches, or both,

defendant is an “aggrieved person” under FISA, and as noted above, he was provided with notice of his status as such and of the Government’s intent to use FISA-obtained or -derived information against him at trial.

⁸ Pub. L. No. 107-56, 115 Stat. 272 (2001).

⁹ As previously noted, FISA defines the term “Attorney General” as the Attorney General of the United States (or Acting Attorney General), the Deputy Attorney General, or, upon the designation by the Attorney General, the Assistant Attorney General for National Security. *See* 50 U.S.C. § 1801(g).

¹⁰ If no FISC order authorizing the electronic surveillance or physical search is issued, emergency surveillance must stop when the information sought is obtained, when the FISC denies an application for an order, or after the expiration of seven days from the time of the emergency employment, whichever is earliest. *See* 50 U.S.C. §§ 1805(e)(3), 1824(e)(3). Moreover, if no FISC order is issued, absent a showing of good cause, the FISC shall cause to be served on any U.S. person named in the application, and others in the FISC’s discretion, notice of the fact of the application, the period of the surveillance, and the fact that during the period information was or was not obtained. *See* 50 U.S.C. § 1806(j); *see also* 50 U.S.C. § 1824(j)(1) (physical searches). In addition, if no FISC order is issued, neither information obtained nor evidence derived from the emergency electronic surveillance or physical search may be disclosed in any court or other proceeding, and no information concerning a United States person acquired from the electronic surveillance or physical search may be used in any other manner by Federal officers or employees without the person’s consent, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm. *See* 50 U.S.C. §§ 1805(e)(5), 1824(e)(5).

within the United States where a significant purpose is the collection of foreign intelligence information.¹¹ 50 U.S.C. §§ 1804(a)(6)(B), 1823(a)(6)(B). Under FISA,

“[f]oreign intelligence information” means

- (1) information that relates to, and if concerning a United States person¹² is necessary to, the ability of the United States to protect against—
 - (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
 - (B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or
 - (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or
- (2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to –
 - (A) the national defense or the security of the United States; or
 - (B) the conduct of the foreign affairs of the United States.

50 U.S.C. § 1801(e). *See also* 50 U.S.C. § 1821(1), adopting the definitions from 50 U.S.C. § 1801. With the exception of emergency authorizations, FISA requires that a court order be obtained before any electronic surveillance or physical searches may be conducted.

An application to conduct electronic surveillance pursuant to FISA must contain, among other things:

- (1) the identity of the federal officer making the application;

¹¹ **CLASSIFIED MATERIAL REDACTED**

¹² **CLASSIFIED MATERIAL REDACTED**

- (2) the identity, if known, or a description of the specific target of the electronic surveillance;
- (3) a statement of the facts and circumstances supporting probable cause to believe that the target is a foreign power or an agent of a foreign power, and that each facility or place at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power;
- (4) a statement of the proposed minimization procedures to be followed;
- (5) a detailed description of the nature of the information sought and the type of communications or activities to be subjected to the surveillance;
- (6) a certification, discussed below, of a high-ranking official;
- (7) the manner or means by which the electronic surveillance will be effected and a statement whether physical entry is required to effect the electronic surveillance;
- (8) the facts concerning and the action taken on all previous FISA applications involving any of the persons, facilities, or places specified in the application; and
- (9) the proposed duration of the electronic surveillance.

50 U.S.C. § 1804(a)(1)-(9).

An application to conduct a physical search pursuant to FISA must contain similar information as an application to conduct electronic surveillance, except that an application to conduct a physical search must also contain a statement of the facts and circumstances supporting probable cause to believe that “the premises or property to be searched contains foreign intelligence information” and that each “premises or property to be searched is or is about to be, owned, used, possessed by, or is in transit to or from” the target. 50 U.S.C. §§ 1823(a)(1-8), (a)(3)(B),(C).

1. The Certification

An application to the FISC for a FISA order must include a certification from a high-ranking executive branch official with national security responsibilities that:

- (A) the certifying official deems the information sought to be foreign intelligence information;
- (B) a significant purpose of the surveillance is to obtain foreign intelligence information;
- (C) such information cannot reasonably be obtained by normal investigative techniques;
- (D) designates the type of foreign intelligence information being sought according to the categories described in [50 U.S.C. §] 1801(e); and
- (E) including a statement of the basis for the certification that –
 - (i) the information sought is the type of foreign intelligence information designated; and
 - (ii) such information cannot reasonably be obtained by normal investigative techniques.

50 U.S.C. § 1804(a)(6). *See also* 50 U.S.C. § 1823(a)(6).

2. Minimization Procedures

The Attorney General has adopted, and the FISC has approved, minimization procedures that regulate the acquisition, retention, and dissemination of non-publicly available information concerning unconsenting United States persons obtained through FISA-authorized electronic surveillance or physical searches, including persons who are not the targets of the FISA authorities. FISA requires that such minimization procedures be:

reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information.

50 U.S.C. §§ 1801(h)(1); 1821(4)(A).

In addition, minimization procedures also include “procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes.” 50 U.S.C. § 1801(h)(3), 1821(4)(c).

CLASSIFIED MATERIAL REDACTED

3. Attorney General’s Approval

FISA further requires that the Attorney General approve applications for electronic surveillance, physical search, or both, before they are presented to the FISC.

C. THE FISC’S ORDERS

Once approved by the Attorney General, the application is submitted to the FISC and assigned to one of its judges. The FISC may approve the requested electronic surveillance, physical searches, or both, only upon finding, among other things, that:

- (1) the application has been made by a “Federal officer” and has been approved by the Attorney General;
- (2) there is probable cause to believe that (A) the target of the electronic surveillance and/or physical search is a foreign power or an agent of a foreign power, and that (B) the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power (or that the premises or property to be searched is, or is about to be, owned, used, possessed by, or is in transit to or from, a foreign power or an agent of a foreign power);
- (3) the proposed minimization procedures meet the statutory requirements set forth in 50 U.S.C. § 1801(h) (electronic surveillance) and 50 U.S.C. § 1821(4) (physical search);
- (4) the application contains all of the statements and certifications required by Section 1804 or Section 1823; and

(5) if the target is a United States person, that the certifications are not clearly erroneous.

50 U.S.C. §§ 1805(a)(1)-(4), 1824(a)(1)-(4).

FISA defines “foreign power” to mean –

- (1) a foreign government or any component, thereof, whether or not recognized by the United States;
- (2) a faction of a foreign nation or nations, not substantially composed of United States persons;
- (3) an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments;
- (4) a group engaged in international terrorism or activities in preparation therefor,
- (5) a foreign-based political organization, not substantially composed of United States persons;
- (6) an entity that is directed and controlled by a foreign government or governments; or
- (7) an entity not substantially composed of United States persons that is engaged in the international proliferation of weapons of mass destruction.

50 U.S.C. §§ 1801(a)(1-7); *See also* 50 U.S.C. § 1821(1), adopting definitions from 50 U.S.C. § 1801.

“Agent of a foreign power” means –

- (1) any person other than a United States person, who—
 - (A) acts in the United States as an officer or employee of a foreign power, or as a member of a foreign power as defined in subsection (a)(4);
 - (B) acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United States, when the circumstances of such person’s

presence in the United States indicate that such person may engage in such activities in the United States, or when such person knowingly aids or abets any person in the conduct of such activities knowingly conspires with any person to engage in such activities;

(C) engages in international terrorism or activities in preparation therefore [sic];

(D) engages in the international proliferation of weapons of mass destruction, or activities in preparation therefor; or

(E) engages in the international proliferation of weapons of mass destruction, or activities in preparation therefor for or on behalf of a foreign power; or

(2) any person who –

(A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States;

(B) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States;

(C) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power;

(D) knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power or, which in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power; or

(E) knowingly aids or abets any person in the conduct of activities described in [the subparagraphs above] . . . or knowingly conspires with any person to engage in activities described in [the subparagraphs above.]

50 U.S.C. §§ 1801(b)(1) and (2); *see also* 50 U.S.C. § 1821(1), adopting definitions from 50 U.S.C. § 1801.

FISA specifies that no United States person may be considered a foreign power or an agent of a foreign power solely on the basis of activities protected by the First Amendment to the Constitution of the United States. 50 U.S.C. §§ 1805(a)(2)(A), 1824(a)(2)(A). Although protected First Amendment activities cannot form the sole basis for FISA-authorized electronic surveillance or physical search, they may be considered by the FISC if there is other activity indicative that the target is an agent of a foreign power. *United States v. Rosen*, 447 F. Supp. 2d 538, 549-50 (E.D. Va. 2006); *United States v. Rahman*, 861 F. Supp. 247, 252 (S.D.N.Y. 1994), *aff'd*, 189 F.3d 88 (2d Cir. 1999). Additionally, FISA provides that “[i]n determining whether or not probable cause exists . . . a judge may consider past activities of the target, as well as facts and circumstances relating to current or future activities of the target.” 50 U.S.C. §§ 1805(b), 1824(b).

If the FISC is satisfied that the FISA application meets the statutory provisions and has made all of the necessary findings, the FISC issues an *ex parte* order authorizing the electronic surveillance, physical searches, or both, requested in the application. 50 U.S.C. §§ 1805(a), 1824(a). The order must specify:

- (1) the identity (or a description of) the specific target of the collection;
- (2) the nature and location of each facility or place at which the electronic surveillance will be directed or of each of the premises or properties that will be searched;
- (3) the type of information sought to be acquired and the type of communications or activities that are to be subjected to the electronic surveillance,

or the type of information, material, or property that is to be seized, altered, or reproduced through the physical search;

(4) the manner and means by which electronic surveillance will be effected and whether physical entry will be necessary to effect that surveillance, or a statement of the manner in which the physical search will be conducted;

(5) the period of time during which electronic surveillance is approved and/or the authorized scope of each physical search; and

(6) the applicable minimization procedures.

50 U.S.C. §§ 1805(c)(1) and 2(A); 1824(c)(1) and 2(A).

The FISC also retains the authority to review, before the end of the authorized period of electronic surveillance or physical searches, the Government's compliance with the requisite minimization procedures. 50 U.S.C. §§ 1805(d)(3), 1824(d)(3).

Under FISA, electronic surveillance or physical searches targeting a United States person may be approved for up to ninety days, and those targeting a non-United States person may be approved for up to one-hundred and twenty days. 50 U.S.C. §§ 1805(d)(1), 1824(d)(1). Extensions may be granted, but only if the United States submits another application that complies with FISA's requirements. An extension for electronic surveillance or physical searches targeting a United States person may be approved for up to ninety days, and one targeting a non-United States person may be approved for up to one year. 50 U.S.C. §§ 1805(d)(2), 1824(d)(2).

III. DISTRICT COURT REVIEW OF FISC ORDERS

FISA authorizes the use in a criminal prosecution of information obtained or derived from any FISA-authorized electronic surveillance or physical search, provided that advance authorization is obtained from the Attorney General, 50 U.S.C. §§ 1806(b),

1825(c), and that proper notice is subsequently given to the court and to each aggrieved person against whom the information is to be used. 50 U.S.C. §§ 1806(c), (d); 1825(d), (e). Upon receiving notice, an aggrieved person against whom the information is to be used may move to suppress the use of the FISA information on two grounds: (1) that the information was unlawfully acquired; or (2) that the electronic surveillance or physical search was not conducted in conformity with an order of authorization or approval. 50 U.S.C. §§ 1806(e), 1825(f). In addition, FISA contemplates that a defendant may file, as Osmakac has done, a motion or request under any other statute or rule of the United States to discover or obtain applications or orders or other materials relating to electronic surveillance or physical searches, *i.e.*, the FISA materials, 50 U.S.C. §§ 1806(f), 1825(g). Whether a defendant moves to suppress FISA information under 50 U.S.C. §§ 1806(e) or 1825(f), or seeks to discover the FISA materials under some other statute or rule, the motion or request is evaluated using FISA's probable cause standard, which is discussed below, and not the probable cause standard applicable to criminal warrants. *See, e.g., United States v. El-Mezain*, 664 F.3d 467, 564 (5th Cir. 2011); *United States v. Duka*, 671 F.3d 329, 336-37 (3d Cir. 2011) (rejecting appellant's challenge to FISA's probable cause standard because it does not require any indication that a crime has been committed); *United States v. Pelton*, 835 F.2d 1067, 1075 (4th Cir. 1987).

A. THE REVIEW IS TO BE CONDUCTED IN CAMERA AND EX PARTE

In assessing the legality of FISA-authorized electronic surveillance, physical searches, or both, the district court, "shall, notwithstanding any other law, if the Attorney General files [as he has filed in this proceeding] an affidavit or declaration under oath

that disclosure or an adversary hearing would harm the national security of the United States, review *in camera* and *ex parte* the application, order, and such other materials relating to the surveillance as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted.”¹³ 50 U.S.C. §§ 1806(f), 1825(g). On the filing of the Attorney General’s affidavit or declaration, the court “may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance or physical search *only where such disclosure is necessary to make an accurate determination of the legality* of the surveillance or search.”¹⁴ 50 U.S.C. §§ 1806(f), 1825(g) (emphasis added). Thus, the propriety of the disclosure of any FISA applications or orders to the defendant cannot even be considered unless and until the district court has first concluded that it is unable to make an accurate determination of the legality of the acquired collection after reviewing the Government’s submissions (and any supplemental pleadings that the district court may request) *in camera* and *ex parte*. See *El-Mezain*, 664 F.3d at 565; *United States v. Abu-Jihaad*, 630 F.3d at 129; *United States v. Belfield*, 692 F.2d 141, 147 (D.C. Cir. 1982); *United States v. Islamic American Relief Agency (IARA)*, No. 07-00087-CR-W-NKL, 2009 WL 5169536, at *3-4 (W.D. Mo. Dec. 21, 2009); *United States v. Nicholson*, No. 09-CR-40-BR, 2010 WL 1641167, at *4 (D.

¹³ **CLASSIFIED MATERIAL REDACTED**

¹⁴ In *United States v. Warsame*, 547 F. Supp. 2d 982, 987 (D. Minn. 2008), the court addressed the meaning of “necessary” in this context: “[t]he legislative history explains that such disclosure is ‘necessary’ only where the court’s initial review indicates that the question of legality may be complicated” by factual misrepresentations, insufficient identification of the target, or failure to comply with the minimization standards in the order.

Or. Apr. 21, 2010) (“After an *in-camera* review, the court ‘has the discretion to disclose portions of the documents, under appropriate protective procedures, *only if [the court] decides that such disclosure is necessary to make an accurate determination of the legality of the surveillance.*’”) (quoting *United States v. Duggan*, 743 F.2d 59, 78 (2d Cir. 1984) (emphasis in *Nicholson*); *United States v. Kashmiri*, 2010 WL 4705159, at *2 (N.D. Ill., Nov. 10, 2010)).¹⁵

If the district court is able to make an accurate determination of the legality of the electronic surveillance, physical searches, or both, based on its *in camera*, *ex parte* review of the materials submitted by the United States, then the court *may not* order disclosure of any of the FISA materials to the defense, unless otherwise required by due process. *El-Mezain*, 664 F.3d at 566; *Duggan*, 743 F.2d at 78; *Kashmiri*, 2010 WL 4705159, at *2.¹⁶

1. *In Camera*, *Ex Parte* Review is the Rule

Federal courts have repeatedly and consistently held that FISA “anticipates that an *ex parte*, *in camera* determination is to be the rule,” with disclosure and an adversarial hearing being the “exception, occurring *only* when necessary.” *Belfield*, 692 F.2d at 147 (emphasis in original); *accord*, *El-Mezain*, 664 F.3d at 567 (“[D]isclosure of FISA materials is the exception and *ex parte*, *in camera* determination is the rule”) (citing *Abu*

¹⁵ The defendant does not contest this interpretation: “A court is required to make an initial *ex parte* review of the FISA applications and orders, then the court is permitted to order disclosure if it finds that it cannot determine the lawfulness of the FISA authority without the assistance of defense counsel or an adversary presentation. 50 U.S.C.A. § 1806(f), § 1825(g), and 1845(f). [sic].” See Defendant’s Motion, Document 121, Defendant’s Motion, ¶ 5.

¹⁶ *Accord*, see Defendant’s Motion, Document 121, ¶ 6.

Jihaad, 630 F.3d 102, 129 (2d. Cir. 2010); *Duggan*, 743 F.2d at 78; *Rosen*, 447 F. Supp. 2d at 546; *Nicholson*, 2010 WL 1641167 at *3-4; *United States v. Spanjol*, 720 F. Supp. 55, 59 (E.D. Pa. 1989), *aff'd*, 958 F.2d 365 (3d Cir. 1992).

In fact, every court that has addressed a motion to disclose FISA materials or to suppress FISA information has been able to reach a conclusion as to the legality of the FISA collection at issue based on its *in camera*, *ex parte* review. *See, e.g., El-Mezain*, 664 F.3d at 566 (quoting district court’s statement that no court has ever held an adversarial hearing to assist the court); *In re Grand Jury Proceedings of the Special Apr. 2002 Grand Jury* (“*In re Grand Jury Proceedings*”), 347 F.3d 197, 203 (7th Cir. 2003) (noting that no court has ever ordered disclosure of FISA materials); *United States v. Isa*, 923 F.2d 1300, 1306 (8th Cir. 1991); *Spanjol*, 720 F. Supp. at 58-59; *United States v. Sattar*, 2003 WL 22137012, at *6 (S.D.N.Y. 2003) (citing *United States v. Nicholson*, 955 F. Supp. 588, 592 & n. 11 (E.D. Va. 1997) (“this court knows of no instance in which a court has required an adversary hearing or disclosure in determining the legality of a FISA surveillance”)), *aff'd*, *U.S. v. Stewart*, 590 F.3d 93 (2d Cir. 2009); *United States v. Thomson*, 752 F. Supp. 75, 79 (W.D.N.Y. 1990); *United States v. Abu-Jihaad*, 531 F. Supp. 2d 299, 310 (D. Conn. 2008), *aff'd*, 630 F.3d at 102, 129-30 (2d Cir. 2010); *United States v. Mubayyid*, 521 F. Supp. 2d 125, 130 (D. Mass. 2007); *Rosen*, 447 F. Supp. 2d at 546; *United States v. Gowadia*, No. 05-00486, 2009 WL 1649714, at *2 (D. Hawaii June 8, 2009); *Kashmiri*, 2010 WL 4705159, at *2-3.

As the Court will see from its examination of the exhibits in the Sealed Appendix, there is nothing extraordinary about the instant FISA-authorized electronic

surveillance and physical searches that would justify this case becoming the first “exception” to the rule of all previous FISA litigation – that is, the first-ever to order the production and disclosure of highly sensitive and classified FISA materials or the suppression of FISA-derived or -obtained evidence. Here, the FISA materials are well-organized and easily reviewable by the Court *in camera* and *ex parte*, and they are fully and facially sufficient to allow the Court to make an accurate determination that the FISA information was lawfully acquired and that the electronic surveillance and physical searches were made in conformity with an order of authorization or approval. The instant materials “are straightforward and readily understood.” *In re Kevork*, 634 F. Supp. 1002, 1008 (C.D. Cal. 1985), *aff’d*, 788 F.2d 566 (9th Cir. 1986). Moreover, as in other cases, “[t]he determination of legality in this case is not complex.” *Belfield*, 692 F.2d at 147; *see also Warsame*, 547 F. Supp. 2d at 987 (“issues presented by the FISA applications are straightforward and uncontroversial”); *Abu-Jihaad*, 531 F. Supp. 2d at 310; *Thomson*, 752 F. Supp. at 79. The Government respectfully submits that this Court, much like the aforementioned courts, is capable of reviewing the FISA materials *in camera* and *ex parte* and making the requisite legal determination without an adversarial hearing.

In addition to the specific harm that would result from the disclosure of the FISA materials in this case, which is detailed in the classified declaration of a high-ranking FBI official in support of the Attorney General’s Declaration and Claim of Privilege, the underlying rationale for non-disclosure is clear: “In the sensitive area of foreign intelligence gathering, the need for extreme caution and sometimes even secrecy may not be overemphasized.” *United States v. Ott*, 827 F.2d 473, 477 (9th Cir. 1987) (“Congress

has a legitimate interest in authorizing the Attorney General to invoke procedures designed to ensure that sensitive security information is not unnecessarily disseminated to *anyone* not involved in the surveillance operation in question.”); *accord*, *IARA*, 2009 WL 5169536, at *3-4.

Confidentiality is critical to national security. “If potentially valuable intelligence sources” believe that the United States “will be unable to maintain the confidentiality of its relationship to them, many [of those sources] could well refuse to supply information.” *CIA v. Sims*, 471 U.S. 159, 175 (1985); *see also*, *Phillippi v. CIA*, 655 F.2d 1325, 1332-33 (D.C. Cir. 1981). When a question is raised as to whether the disclosure of classified sources, methods, techniques, or information would harm the national security, federal courts have expressed a great reluctance to replace the considered judgment of Executive Branch officials charged with the responsibility of weighing a variety of subtle and complex factors in determining whether the disclosure of information may lead to an unacceptable risk of compromising the intelligence gathering process, and determining whether foreign agents, spies, and terrorists are capable of piecing together a mosaic of information that, when revealed, could reasonably be expected to harm the national security of the United States. *See Sims*, 471 U.S. at 180; *United States v. Yunis*, 867 F.2d 617, 623 (D.C. Cir. 1989) (“Things that did not make sense to the District Judge would make all too much sense to a foreign counter-intelligence specialist who could learn much about this nation’s intelligence-gathering capabilities from what these documents revealed about sources and methods.”); *Halperin v. CIA*, 629 F.2d 144, 150 (D.C. Cir. 1980) (“each individual piece of intelligence information, much like a piece of jigsaw

puzzle, may aid in piecing together other bits of information even when the individual piece is not of obvious importance in itself”). An adversary hearing is not only unnecessary to aid the Court in the straightforward task before it, but such a hearing would *create* potential dangers that courts have consistently sought to avoid.

As the *Belfield* court explained:

Congress recognized the need for the Executive to engage in and employ the fruits of clandestine surveillance without being constantly hamstrung by disclosure requirements. The statute is meant to “reconcile national intelligence and counterintelligence needs with constitutional principles in a way that is consistent with both national security and individual rights.” In FISA the privacy rights of individuals are ensured not through mandatory disclosure, but through its provisions for in-depth oversight of FISA surveillance by all three branches of government and by a statutory scheme that to a large degree centers on an expanded conception of minimization that differs from that which governs law enforcement surveillance.

692 F.2d at 148 (footnotes and citations omitted); *see also* *ACLU Found. of So. Cal. v. Barr* (“*ACLU Foundation*”), 952 F.2d 457, 465 (D.C. Cir. 1991) (citing *Belfield* for the proposition that Section 1806(f) “is an acceptable means of adjudicating the constitutional rights of persons who have been subjected to FISA surveillance”).

2. In Camera, Ex Parte Review is Constitutional

The constitutionality of FISA’s *in camera, ex parte* review provisions has been affirmed by every federal court that has considered the matter. *See, e.g., El-Mezain*, 664 F.3d at 567; *Abu-Jihaad*, 630 F.3d at 117; *Spanjol*, 720 F. Supp. at 58-59; *United States v. Damrah*, 412 F.3d 618, 624 (6th Cir. 2005) (“FISA’s requirement that the district court conduct an *ex parte, in camera* review of FISA materials does not deprive a defendant of

due process.”); *Ott*, 827 F.2d at 476-77 (FISA’s review procedures do not deprive a defendant of due process); *Gowadia*, 2009 WL 1649714, at *2; *United States v. Jayyousi*, No. 04-60001, 2007 WL 851278, at *7-8 (S.D. Fla. Mar. 15, 2007), *aff’d*, 657 F.3d 1085 (11th Cir. 2011);¹⁷ *United States v. Benkahla*, 437 F. Supp. 2d 541, 554 (E.D. Va. 2006); *ACLU Foundation*, 952 F.2d at 465; *United States v. Megahey*, 553 F. Supp. 1180, 1194 (E.D.N.Y. 1982) (“*ex parte*, *in camera* procedures provided in 50 U.S.C. § 1806(f) are constitutionally sufficient to determine the lawfulness of the electronic surveillance at issue while safeguarding defendants’ fourth amendment rights”); *United States v. Falvey*, 540 F. Supp. 1306, 1315-16 (E.D.N.Y. 1982) (a “massive body of pre-FISA case law of the Supreme Court, [the Second] Circuit and others” supports the conclusion that the legality of electronic surveillance should be determined on an *in camera*, *ex parte* basis); *Belfield*, 692 F.2d at 148-49; *Nicholson*, 2010 WL 1641167, at *3-4.

There remains an unbroken history of federal court holdings that FISA’s *in camera*, *ex parte* review provisions are entirely compatible with the requirements and protections of the Constitution. As stated by the United States District Court for the Northern District of Georgia, “[t]he defendants do not cite to any authority for [the proposition that FISA is unconstitutional] because there is none. Every court that has considered FISA’s constitutionality has upheld the statute from challenges under the *Fourth, Fifth, and Sixth Amendments*.” *United States v. Ahmed*, No. 1:06-CR-147-WSD-CGB, 2009 U.S. Dist. LEXIS 120007, at *30 (N.D. Ga. Mar. 19, 2009) (order denying defendants’ motion to disclose and suppress FISA materials).

¹⁷ All citations to *Jayyousi* herein are to the Magistrate Judge’s Report and Recommendation which was adopted and incorporated into the Court’s Opinion.

In summary, FISA mandates a process by which the district court must conduct an initial *in camera, ex parte* review of FISA applications, orders, and related materials in order to determine whether the FISA information was lawfully acquired and whether the surveillance and searches were made in conformity with an order of authorization or approval. Such *in camera, ex parte* review is the rule in such cases and that procedure is constitutional. In this case, the Attorney General has filed the required declaration invoking that procedure, and has declared that disclosure or an adversary hearing would harm national security. Accordingly, an *in camera, ex parte* review by this Court is the appropriate venue in which to determine whether the FISA information was lawfully acquired and whether the surveillance and searches were made in conformity with an order of authorization or approval.

B. THE DISTRICT COURT'S SUBSTANTIVE REVIEW

1. Standard of Review of Probable Cause

In evaluating the legality of the FISA collection, the district court's review should determine: (1) whether the certification submitted by the Executive Branch in support of a FISA application was properly made; (2) whether the application established the probable cause required by FISA; and (3) whether the collection was properly minimized. *See Abu-Jihaad*, 630 F.3d at 130-31. *See also* 50 U.S.C. §§ 1806(f), 1825(g).

Although federal courts are not in agreement as to whether the probable cause determinations of the FISC should be reviewed *de novo* or accorded due deference, the material under review here satisfies the higher standard of *de novo* review. *See Abu-Jihaad*, 630 F.3d at 130 (“Although the established standard of judicial review applicable

to FISA warrants is deferential, the government’s detailed and complete submissions in this case would easily allow it to clear a higher standard of review.”) Understanding that the Eleventh Circuit has not addressed the standard of review applicable in this matter, the Government respectfully submits that it is appropriate to accord due deference to the findings of the FISC, but notes that a number of courts have declined to do so, citing the *ex parte* nature of the proceedings, and have instead reviewed the FISC’s probable cause determination *de novo*.¹⁸ While in the minority, other courts, including the Second Circuit in *Abu-Jihaad* 630 F.3d at 130, have afforded due deference to the findings of the FISC; *accord Ahmed*, 2009 U.S. Dist. LEXIS 120007, at *21-22 (FISC’s “determination of probable cause should be given ‘great deference’ by the reviewing court”) (citing *Illinois v. Gates*, 462 U.S. at 236).

In the analogous area of criminal searches and surveillance, the law in the Eleventh Circuit accords great deference to a magistrate judge’s probable cause determinations. *See, e.g., United States v. Joseph*, 709 F. 3d 1082, 1093 (11th Cir. 2013). It would thus be consistent for a court that is reviewing FISC-authorized physical searches and electronic surveillance to adopt the same posture it would when reviewing the probable cause determination of a criminal search warrant issued pursuant to Rule 41 of the Federal Rules of Criminal Procedure. *See Ahmed*, 2009 U.S. Dist. LEXIS 120007, at *21-22 (accord FISC’s probable cause determinations the same deference as a magistrate’s criminal probable cause determination).¹⁹

¹⁸ **CLASSIFIED MATERIAL REDACTED**

¹⁹ *Ahmed* is not alone in analogizing FISA applications to criminal search warrants. *See, e.g., United States v. Cavanagh*, 807 F.2d 787, 790 (9th Cir. 1987) (concluding that FISA order can be considered a

FISA requires a finding of probable cause that the target is a foreign power or an agent of a foreign power and that each facility or place at which the electronic surveillance is directed is being used, or is about to be used, or that property or premises to be searched is, or is about to be, owned, used, possessed by, or is in transit to or from, a foreign power or an agent of a foreign power. It is this standard, not the standard applicable to criminal search warrants, that this Court must apply. *See El-Mezain*, 664 F.3d at 564 (“[t]his probable cause standard is different from the standard in the typical criminal case because, rather than focusing on probable cause to believe that a person has committed a crime, the FISA standard focuses on the status of the target as a foreign power or an agent of a foreign power”); *Abu-Jihaad*, 630 F.3d at 130-31; *Duka*, 671 F.3d at 338; *Cavanagh*, 807 F.2d. at 790 (citing *United States v. United States District Court (Keith)*, 407 U.S. 297, 322 (1972)). This “different, and arguably lower, probable cause standard . . . reflects the purpose for which FISA search orders are issued.” *Ahmed*, 2009 U.S. Dist. LEXIS 120007, at *22.

CLASSIFIED MATERIAL REDACTED

2. Standard of Review of Certifications

Certifications submitted in support of a FISA application should be “subjected only to minimal scrutiny by the courts,” *United States v. Badia*, 827 F.2d 1458, 1463 (11th Cir. 1987), and are “presumed valid.” *Duggan*, 743 F.2d at 77 & n.6 (citing *Franks v. Delaware*, 438 U.S. 154, 171 (1978)); *United States v. Campa*, 529 F.3d 980, 993

warrant since it is issued by a detached judicial officer and is based on a reasonable showing of probable cause); *In Re Sealed Case*, 310 F.3d 717, 742 (FISC of Rev. 2002) (declining to decide whether a FISA order constitutes a warrant, but noting “that to the extent a FISA order comes close to meeting Title III, that certainly bears on its reasonableness under the Fourth Amendment”).

(11th Cir. 2008); *United States v. Sherifi*, 793 F. Supp. 2d 751, 760 (E.D. N.C. 2011) (“a presumption of validity [is] accorded to the certifications”); *Nicholson*, 2010 WL 1641167, at *5 (quoting *Rosen*, 447 F. Supp. 2d at 545); *Warsame*, 547 F. Supp. 2d at 990 (“a presumption of validity [is] accorded to the certifications”). When a FISA application is presented to the FISC, “[t]he FISA Judge, in reviewing the application, is not to second-guess the executive branch official’s certification that the objective of the surveillance is foreign intelligence information.” *Duggan*, 743 F.2d at 77. Likewise, Congress intended that the reviewing district court should “have no greater authority to second-guess the executive branch’s certifications than has the FISA judge.” *Id.*; see also *In re Grand Jury Proceedings*, 347 F.3d at 204-05; *Badia*, 827 F.2d at 1463; *Rahman*, 861 F. Supp. at 250; *IARA*, 2009 WL 5169536, at *4; *Kashmiri*, 2010 WL 4705159, at *1.

The district court’s review should determine whether the certifications were made in accordance with FISA’s requirements. See *United States v. Alwan*, No. 1:11-CR-13-R, 2012 WL 399154, at *7 (W.D. Ky. Feb. 7, 2012) (“the [c]ourt is not to second-guess whether the certifications were correct, but merely to ensure they were properly made’) (quoting *Ahmed*, 2009 U.S. Dist. LEXIS 120007, at *20); see also *Campa*, 529 F.3d at 993 (“in the absence of a *prima facie* showing of a fraudulent statement by the certifying officer, procedural regularity is the only determination to be made if a non-United States person is the target”) (quoting *Badia*, 837 F.2d at 1463). When the target is a United States person, then the district court should also ensure that each certification is not “clearly erroneous.” *Id.* at 994; *Duggan*, 743 F.2d at 77; *Kashmiri*, 2010 WL 4705159, at

*2. A certification is clearly erroneous only when “the reviewing court on the [basis of the] entire evidence is left with the definite and firm conviction that a mistake has been committed.” *United States v. U.S. Gypsum Co.*, 333 U.S. 364, 395 (1948); *see also United States v. Garcia*, 413 F.3d 201, 222 (2d Cir. 2005); *IARA*, 2009 WL 5169536, at *4.

3. FISA is Subject to the “Good-Faith” Exception

Even assuming *arguendo* that this Court determines that a particular FISC order was not supported by probable cause, or that one or more of the FISA certification requirements were not in fact met, the Government respectfully submits that the evidence obtained or derived from the FISA-authorized electronic surveillance and physical searches is, nonetheless, admissible under the “good faith” exception to the exclusionary rule articulated in *United States v. Leon*, 468 U.S. 897 (1984).²⁰ The Seventh Circuit, relying on *Leon*, held that federal officers were entitled to rely in good faith on a FISA warrant. *United States v. Ning Wen*, 477 F.3d 896, 897 (7th Cir. 2007). As the court noted:

[T]he exclusionary rule must not be applied to evidence seized on the authority of a warrant, even if the warrant turns out to be defective, unless the affidavit supporting the warrant was false or misleading, or probable cause was so transparently missing that “no reasonably well trained officer [would] rely on the warrant.”

²⁰ “[E]ven if we were to conclude that amended FISA is unconstitutional, evidence derived from it would nevertheless have been admissible in the government’s case. . . . The exclusionary rule precludes the admission of evidence tainted by a Fourth Amendment violation” only in those cases where its application will deter police misconduct. *Duka*, 671 F.3d at 346 (citing *Leon*, 468 U.S. at 918).

Id. (quoting *Leon*) (alteration in original); *see also Duggan*, 743 F.2d at 77 n.6 (*Franks* principles apply to review of FISA orders); *Ahmed*, 2009 U.S. Dist. LEXIS 120007, at *25 n.8, 26-27 (“[t]he FISA evidence obtained . . . would be admissible under *Leon*’s ‘good faith’ exception to the exclusionary rule were it not otherwise admissible under a valid warrant”).

The FISA-authorized electronic surveillance and physical searches at issue in this case would fall squarely within this “good faith exception.” There is no basis to find that any declarations or certifications at issue in this case were deliberately or recklessly false. *See Leon*, 468 U.S. at 914-15; *see also Massachusetts v. Sheppard*, 468 U.S. 981 (1984); *United States v. Canfield*, 212 F.3d 713, 717-18 (2d Cir. 2000). Further, there are no facts indicating that the FISC failed to act in a neutral and detached manner in authorizing the surveillance and searches at issue. *Leon*, 468 U.S. at 914-15. Moreover, as the Court will see from its *in camera*, *ex parte* review of the FISA materials, facts establishing the requisite probable cause were submitted to the FISC, the FISC’s orders contained all of the requisite findings, and “well-trained officers” reasonably relied on those orders. Therefore, in the event that the Court questions whether a particular FISC order was supported by sufficient probable cause, the information obtained pursuant to those orders would be admissible under *Leon*’s “good faith” exception to the exclusionary rule.

C. **THE COURT SHOULD NOT DISCLOSE THE FISA MATERIALS TO THE DEFENDANT**

Defendant’s motion seeks the disclosure of the classified FISA materials, which are protected from such disclosure, except as provided in 50 U.S.C. §§ 1806(f)-(g) and

1825 (g)-(h) (*i.e.*, if necessary for the Court to make a determination of the legality of the electronic surveillance or physical search, or if due process requires discovery or disclosure).²¹

The Court’s *in camera*, *ex parte* review does not violate due process, nor does due process require that Osmakac be granted access to the FISA materials except as provided for in §§ 1806(f)-(g) and 1825 (g)-(h).²² A challenge that FISA’s *ex parte*, *in camera* review violates the Sixth Amendment’s right to confrontation was specifically rejected in *Isa*, 923 F.2d at 1306-07, where the court ruled that the right of confrontation is “not absolute” and may bow to accommodate legitimate interests in the criminal trial process, and that, given the substantial interests at stake and the protections provided, the defendant’s Sixth Amendment rights were not violated. Similar Sixth Amendment arguments were advanced unsuccessfully in *Warsame*. 547 F. Supp. 2d at 988 n.4 (citing to *Nicholson*, 955 F. Supp. at 592); *Belfield*, 692 F.2d at 148; *Megahey*, 553 F. Supp. at 1193; *Benkhala*, 437 F. Supp. 2d at 554; *Nicholson*, 955 F. Supp. 592 & n.11; *Falvey*, 540 F. Supp. at 1315-16 (rejecting challenges under the First, Fifth, and Sixth Amendments). As summarized by the United States District Court for the Northern District of Georgia, “[t]he defendants do not cite to any authority for [the proposition that

²¹ It should be noted that two distinct due process considerations are relevant. First, whether the Court’s *in camera*, *ex parte* review of the challenged FISA materials under §§ 1806(f) and 1825 (g) accords with due process, which, as discussed below, it does. Second, whether the Court’s *in camera*, *ex parte* review of the challenged FISA materials reveals information contained therein that due process requires be disclosed to the defendant, such as *Brady* material, as provided for in §§ 1806 (g) and 1825(h). It is clear that the second consideration is a factual one, which the Court will not confront until it has conducted its *in camera*, *ex parte* review of the FISA materials.

²² See, e.g., *Abu Jihaad*, 630 F.3d at 129; *Damrah*, 412 F.3d at 624; *Ott*, 827 F.2d at 476-77; *ACLU Foundation*, 952 F.2d at 465; *Spanjol*, 720 F.Supp. at 58; *Gowadia*, 2009 U.S. Dist. LEXIS 47833, at *6; *United States v. Jayyousi*, No. 04-60001-CR, 2007 WL 851278, at *7; *Falvey*, 540 F. Supp. at 1315.

FISA is unconstitutional] because there is none. Every court that has considered FISA's constitutionality has upheld the statute from challenges under the Fourth, Fifth, and Sixth Amendments." *Ahmed*, No. 1:06-CR-147-WSD-CGB, 2009 U.S. Dist. Lexis 120007, at *30.

The defendant's lack of access to any FISA application or order cannot form a substitute basis for the Court to order disclosure. Despite the quandary defense counsel inevitably face when notified that FISA-obtained or -derived information will be used against a defendant, Congress mandated, and the courts have recognized, that this quandary does not justify the disclosure of FISA materials:

We appreciate the difficulties of appellants' counsel in this case. They must argue that the determination of legality is so complex that an adversary hearing with full access to relevant materials is necessary. But without access to relevant materials their claim of complexity can be given no concreteness. It is pure assertion.

Congress was also aware of these difficulties. But it chose to resolve them through means other than mandatory disclosure. In FISA Congress has made a thoroughly reasonable attempt to balance the competing concerns of individual privacy and foreign intelligence Appellants are understandably reluctant to be excluded from the process whereby the legality of a surveillance by which they were incidentally affected is judged. But it cannot be said that this exclusion rises to the level of a constitutional violation.

Belfield, 692 F.2d at 148. *See also Mubayyid*, 521 F. Supp. 2d at 131 (quoting *Belfield*).

As noted above, every court that has addressed a motion to disclose FISA materials has denied the motion and determined the legality of the FISA collection based on an *in camera*, *ex parte* review. The Government respectfully submits that there is nothing extraordinary about this case that would prompt this Court to be the first to order

the disclosure of highly sensitive and classified FISA materials. Disclosure is simply not necessary in order for the Court to determine the legality of the FISA collections at issue. Congress' clear intention is that the FISA materials should be reviewed *in camera* and *ex parte*, and in a manner consistent with the realities of modern intelligence needs and investigative techniques.

Indeed, the Attorney General has filed a declaration in this case stating that disclosure or an adversary hearing would harm the national security of the United States. *See* Sealed Exhibit 1. Therefore, FISA mandates that this Court conduct an *in camera*, *ex parte* review of the challenged FISA materials to determine whether the collection at issue was both lawfully acquired and lawfully conducted. In conducting that review, the Court may disclose the FISA materials "only where such disclosure is necessary to make an accurate determination of the legality of the surveillance [or search]." ²³ *See* 50 U.S.C. §§ 1806(f) and 1825(g). Congress, in enacting FISA's procedures for *in camera*, *ex parte* judicial review, has balanced and accommodated the competing interests of the Government and criminal defendants, and has articulated the proper standard for disclosure; that is, only where the Court finds that disclosure is necessary to the Court's accurate determination of the legality of the FISA collection. *See id.* The Government submits that the Court will be able to render a determination based on its *in camera*, *ex parte* review, and the defendant expressly agrees with this process. *See* Defendant's Motion, Document 121, paragraph 1.

²³ The defendant does not challenge the procedure whereby the Court conducts an *in camera*, *ex parte* review of the challenged FISA materials, with disclosure being appropriate only if the Court cannot determine the legality of the relevant electronic surveillance and physical searches without the assistance of defense counsel. *See* Document 121, Defendant's Motion, ¶ 3.

CLASSIFIED MATERIAL REDACTED

IV. THE FISA INFORMATION WAS LAWFULLY ACQUIRED AND
THE ELECTRONIC SURVEILLANCE AND PHYSICAL SEARCHES
WERE MADE IN CONFORMITY WITH AN ORDER OF
AUTHORIZATION OR APPROVAL

CLASSIFIED MATERIAL REDACTED.

A. THE INSTANT FISA APPLICATIONS MET FISA'S PROBABLE
CAUSE STANDARD

CLASSIFIED MATERIAL REDACTED

1. CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED

2. CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED

a. CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED

b. CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED

c. CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED

d. CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED

i. CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED

ii. CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED

iii. CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED

e. CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED

3. CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED

4. CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED

a. CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED

b. CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED

c. CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED

d. CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED

e. CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED

f. CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED

g. CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED

h. CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED

5. CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED

6. CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED

a. CLASSIFIED MATERIAL REDACTED

i. CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED

ii. CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED

iii CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED

b. CLASSIFIED MATERIAL REDACTED

i. CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED

ii. CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED

iii. CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED

iv. CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED

c. CLASSIFIED MATERIAL REDACTED

i. CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED

ii. CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED

iii. CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED

iv. CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED

v. CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED

vi. CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED

vii. CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED

d. CLASSIFIED MATERIAL REDACTED

i. CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED

ii. CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED

iii. CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED

iv. CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED

v. CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED

vi. CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED

vii. CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED

viii. CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED

ix. CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED

x. CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED

xi. CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED

xii. CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED

xiii. CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED

e. CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED

i. CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED

f. CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED

i. CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED

ii. CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED

iii. CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED

iv. CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED

v. CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED

vi. CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED

g. CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED

i. CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED

ii. CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED

iii. CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED

iv. CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED

7. Conclusion: There was Sufficient Probable Cause to Establish that the Electronic Surveillance and Physical Searches Were Lawfully Authorized

CLASSIFIED MATERIAL REDACTED

B. THE CERTIFICATIONS COMPLIED WITH FISA

CLASSIFIED MATERIAL REDACTED

1. Foreign Intelligence Information

CLASSIFIED MATERIAL REDACTED

2. “A Significant Purpose”

CLASSIFIED MATERIAL REDACTED

3. Information Not Reasonably Obtainable Through Normal Investigative Techniques

CLASSIFIED MATERIAL REDACTED

For all of the above reasons, the FISC correctly found that the certifications were not clearly erroneous.

C. THE ELECTRONIC SURVEILLANCE AND PHYSICAL SEARCHES WERE MADE IN CONFORMITY WITH AN ORDER OF AUTHORIZATION OR APPROVAL

This Court's *in camera*, *ex parte* review of the FISA materials will demonstrate not only that the FISA collection was lawfully authorized, but also that it was made in conformity with an order of authorization or approval (*i.e.*, lawfully conducted). That is, the FISA-obtained or -derived information that will be offered into evidence in this case was acquired, retained, and disseminated by the FBI in accordance with FISA's minimization requirements and the implementing SMPs adopted by the Attorney General and approved by the FISC.

1. The Standard Minimization Procedures

If a reviewing court is satisfied that the electronic surveillance or physical searches were properly certified and lawfully authorized pursuant to FISA, it must then examine whether the electronic surveillance or physical searches were lawfully conducted. *See* 50 U.S.C. §§ 1806(e)(2), 1825(f)(1)(B). In order to determine whether the electronic surveillance or physical searches were lawfully conducted, the reviewing court must examine whether the Government followed the relevant minimization procedures to appropriately minimize the information acquired, retained, and disseminated pursuant to FISA.

CLASSIFIED MATERIAL REDACTED

FISA’s legislative history and the applicable case law demonstrate that the definitions of “minimization procedures” and “foreign intelligence information” were intended to take into account the realities of collecting foreign intelligence involving the activities of persons engaged in clandestine intelligence gathering or international terrorism that are often not obvious on their face. *See Rahman*, 861 F. Supp. at 252-53. The degree to which information is required to be minimized varies somewhat given the specifics of a particular investigation, such that less minimization at acquisition is justified when “the investigation is focusing on what is thought to be a widespread conspiracy” and more extensive surveillance is necessary “to determine the precise scope of the enterprise.” *In re Sealed Case*, 310 F.3d at 741; *see also United States v. Bin Laden*, 126 F. Supp. 2d 264, 286 (S.D. N.Y. 2000) (“more extensive monitoring and greater leeway in minimization efforts are permitted in a case like this given the world-wide, covert and diffuse nature of the international terrorist group(s) targeted” (internal quotation marks omitted)). Furthermore, the activities of foreign powers and their agents are often not obvious from an initial or cursory overhear of conversations. To the contrary, agents of foreign powers frequently engage in coded communications, compartmentalized operations, the use of false identities, and other practices designed to conceal the breadth and aim of their operations, organization, activities, and plans. *See, e.g., United States v. Salameh*, 152 F.3d 88, 154 (2d Cir. 1998) (noting that two conspirators involved in the 1993 bombing of the World Trade Center in New York referred to the bomb plot as the “study” and to terrorist materials as “university papers”). As one court explained, “[i]nnocuous-sounding conversations may in fact be signals of

important activity; information on its face innocent when analyzed or considered with other information may become critical.” *Kevork*, 634 F. Supp. at 1017 (quoting H.R. Rep. No. 95-1283, 95th Cong., 2d Sess., Pt. 1 at 5 (1978) (hereinafter “House Report”)); *see also Hammoud*, 381 F.3d at 334 (citing *Salameh*, 152 F.3d at 154); *In re Sealed Case*, 310 F.3d at 740-41; *Thomson*, 752 F. Supp. at 81 (noting that it is permissible to retain and disseminate “bits and pieces” of information until the information’s “full significance becomes apparent”; citing House Report, part 1, at 58); *Bin Laden*, 126 F. Supp. 2d at 286. Likewise, “individual items of information, not apparently significant when taken in isolation, may become highly significant when considered together over time.” *Rahman*, 861 F. Supp. at 252-53 (citing House Report, part 1, at 55, 59). The Government must also be given flexibility when the conversations are conducted in a foreign language. *Mubayyid*, 521 F. Supp. 2d at 134; *Rahman*, 861 F. Supp. at 252. As a result, “courts have construed ‘foreign intelligence information’ broadly and sensibly allowed the government some latitude in its determination of what is foreign intelligence information.” *Rosen*, 447 F. Supp. 2d at 551.

The nature of the foreign intelligence information sought also impacts implementation of the minimization procedures at the retention and dissemination stages. There is a legitimate need to conduct a thorough post-acquisition review of FISA information that involves a United States person who is acting as an agent of a foreign power. Congress explained that:

It is “necessary” to identify anyone working with him in this network, feeding him information, or to whom he reports. Therefore, it is necessary to acquire, retain and disseminate information concerning all his contacts and acquaintances and his movements. Among his contacts and

acquaintances, however, there are likely to be a large number of innocent persons. Yet, information concerning these persons must be retained at least until it is determined that they are not involved in the clandestine intelligence activities and may have to be disseminated in order to determine their innocence.

House Report, part 1, at 58. Indeed, at least one court has cautioned that when a United States person communicates with an agent of a foreign power, the Government would be “remiss in meeting its foreign counterintelligence responsibilities” if it did not thoroughly “investigate such contacts and gather information to determine the nature of those activities.” *Thomson*, 752 F. Supp. at 82.

Congress also recognized that agents of a foreign power are often very sophisticated and skilled at hiding their activities. *Cf.*, *Thomson*, 752 F. Supp. at 81 (quoting House Report part 1, at 58). Accordingly, to pursue leads, Congress intended that the Government be given “a significant degree of latitude” with respect to the “retention of information and the dissemination of information between and among counterintelligence components of the Government.” *Cf.*, *Thomson*, 752 F. Supp. at 81 (quoting House Report part 1, at 58).

In light of these realities, Congress recognized that “no electronic surveillance can be so conducted that innocent conversations can be totally eliminated.” *See* S. Rep. No. 95-701, 95th Cong., 2d Sess., 39 (quoting *Keith*, 407 U.S. at 323) (1978) (“Senate Report”). The Fourth Circuit reached the same conclusion in *Hammoud*, stating that the “mere fact that innocent conversations were recorded, without more, does not establish that the government failed to appropriately minimize surveillance.” 381 F.3d at 334.

Accordingly, in reviewing the adequacy of minimization efforts, the test to be applied is neither whether innocent conversations were intercepted, nor whether mistakes were made with respect to particular communications. Rather, as the United States Supreme Court stated in the context of Title III surveillance, there should be an “objective assessment of the [agents’] actions in light of the facts and circumstances confronting [them] at the time.” *Scott v. United States*, 436 U.S. 128, 136 (1978). “The test of compliance is ‘whether a good-faith effort to minimize was made.’” *Mubayyid*, 521 F.Supp.2d at 135. *See also, Hammoud*, 381 F.3d at 334 (“[t]he minimization requirement obligates the Government to make a good faith effort to minimize the acquisition and retention of irrelevant information”); *see also*, Senate Report at 39-40 (stating that the court’s role is to determine whether “on the whole, the agents have shown a high regard for the right of privacy and have done all they reasonably could do to avoid unnecessary intrusion”); *IARA*, 2009 WL 5169536, at *6 (quoting Senate Report at 39-40).

Moreover, as noted above, FISA expressly states that the Government is not required to minimize information that is “evidence of a crime,” whether or not it is also foreign intelligence information. 50 U.S.C. §§ 1801(h)(3), 1821(4)(c); *see also, Isa*, 923 F.2d at 1304 (noting that “[t]here is no requirement that the ‘crime’ be related to foreign intelligence”). As a result, to the extent that certain communications of a United States person may be evidence of a crime or otherwise may establish an element of a substantive or conspiratorial offense, such communications need not be minimized. *See, Isa*, 923 F.2d at 1305.

Even assuming, *arguendo*, that certain communications were not properly minimized, suppression would not be the appropriate remedy with respect to those communications that met the standard. *Cf. United States v. Falcone*, 364 F. Supp. 877, 886-87 (D.N.J. 1973), *aff'd*, 500 F.2d 1401 (3d Cir. 1974) (Title III). As discussed above, absent evidence that “on the whole” there has been a “complete” disregard for the minimization procedures, the fact that some communications should have been minimized does not affect the admissibility of others that were properly acquired and retained. Indeed, Congress specifically intended that the only evidence that should be suppressed is any “evidence which was obtained unlawfully.” House Report at 93. FISA’s legislative history reflects that Congress intended only a limited sanction for errors of minimization:

As the language of the bill makes clear, only that evidence which was obtained unlawfully or derived from information obtained unlawfully would be suppressed. If, for example, some information should have been minimized but was not, only that information should be suppressed; the other information obtained lawfully should not be suppressed.

Id.; see also *Falcone*, 364 F. Supp. at 886-87; accord, *United States v. Medunjanin*, No. 10 CR 19 1 (RJD), 2012 WL 526428, at *12 (S.D. N.Y. Feb. 16, 2012) (disclosure and suppression not warranted where “failure to adhere to [the minimization] protocol was *de minimis*”).

2. The FISA Information was Appropriately Minimized

CLASSIFIED MATERIAL REDACTED

Based upon this information, we respectfully submit that the Government lawfully conducted the FISA collection at issue herein. Consequently, for the reasons

stated above, the Court should find that the FISA-authorized collection at issue in this case was lawfully conducted under the minimization procedures approved by the FISC.

V. CONCLUSION

The defendant's discovery motion should be denied. Courts have uniformly held that the probable cause requirement of FISA comports with the requirements of the Fourth Amendment to the United States Constitution, *see, e.g., Isa*, 923 F.2d at 1304; and that FISA's provisions for *in camera*, *ex parte* review comport with the due process requirements of the United States Constitution. *See, e.g., Spanjol*, 720 F. Supp. at 58-59; *United States v. Butenko*, 494 F.2d 593, 607 (3d Cir.), *cert denied sub nom., Ivanov v. United States*, 419 U.S. 881 (1974); *Damrah*, 412 F.3d at 624; *Warsame*, 547 F. Supp. 2d at 988-89. The defendant advances no argument to justify any deviation from this well-established precedent.

Furthermore, the Court's examination of the materials in the Sealed Appendix will demonstrate that the Government satisfied FISA's requirements to obtain orders for electronic surveillance, physical searches, or both, and the information obtained pursuant to FISA authorities was lawfully acquired and that the electronic surveillance and physical searches were made in conformity with an order of authorization or approval (*i.e.*, lawfully conducted).

Even if this Court were to determine that the acquisition of the FISA collection had not been lawfully acquired or lawfully conducted, the FISA-obtained or -derived evidence would nevertheless be admissible under the "good faith" exception to the exclusionary rule articulated in *Leon*, 468 U.S. 897 (1984). *See also, Ning Wen*, 477 F.3d

at 897 (holding that the *Leon* good-faith exception applies to FISA orders); *Mubayyid*, 521 F. Supp. 2d at 140 n. 12 (noting that the Government could proceed in good-faith reliance on FISA orders even if FISA were deemed unconstitutional); *Ahmed*, 2009 U.S. Dist. LEXIS 120007, at *25 n. 8; *Nicholson*, 2010 WL 1641167, at *6.

The Attorney General has filed a declaration in this case stating that disclosure or an adversary hearing would harm the national security of the United States. Therefore, FISA mandates that this Court conduct an *in camera*, *ex parte* review of the challenged FISA materials to determine whether the collection was lawfully acquired. In conducting that review, the Court may disclose the FISA materials “only where such disclosure is necessary to make an accurate determination of the legality of the surveillance [or search].” 50 U.S.C. §§ 1806(f), 1825(g). Congress, in enacting FISA’s procedures for *in camera*, *ex parte* judicial review, has balanced and accommodated the competing interests of the Government and criminal defendants, and has articulated the proper standard for disclosure; that is, only where the Court finds that disclosure is necessary to the Court’s accurate determination of the legality of the FISA collection.

The Government respectfully submits that the Court can make this determination without disclosing the classified and highly sensitive FISA materials to the defendant. Every federal court that has been asked to determine the legality of a FISA-authorized collection has been able to do so *in camera*, *ex parte* and without the assistance of defense counsel. The FISA materials at issue here are organized and readily understood, and an overview of them is presented herein as a frame of reference. This Court will be able to render a determination based on its *in camera*, *ex parte* review, and the defendant

has failed to present any colorable basis for supplanting Congress' reasoned judgment with a different proposed standard of review.

Based on the foregoing analysis, the Government respectfully submits that the Court should: (1) conduct an *in camera, ex parte* review of the FISA materials and the Government's classified submission; (2) find that the electronic surveillance and physical searches at issue in this case were both lawfully authorized and lawfully conducted in compliance with the Fourth Amendment; (3) hold that disclosure to the defendant of the FISA materials and the Government's classified submissions is not authorized because the Court is able to make an accurate determination of the legality of the surveillance without disclosing the FISA materials or any portions thereof; (4) order that the FISA materials and the Government's classified submissions be maintained under seal by the

Classified Information Security Officer or his or her designee; and (5) deny the defendant's discovery request to the extent that it seeks disclosure of FISA materials.²⁴

DATED: June 14, 2013

Respectfully submitted,

ROBERT E. O'NEILL
United States Attorney

By: *s/Sara C. Sweeney*
Sara C. Sweeney
Assistant United States Attorney
United States Attorney No. 0000119
400 N. Tampa St., Suite 3200
Tampa, Florida 33602
Telephone (813) 274-6000
Facsimile (813) 274-6178
sara.sweeney@usdoj.gov

Clement McGovern
Trial Attorney
Counterterrorism Section
National Security Division
U.S. Department of Justice

²⁴ A district court order granting motions or requests under 50 U.S.C. § 1806(g), a decision that electronic surveillance was not lawfully authorized or conducted, and an order requiring the disclosure of FISA materials is a final order for purposes of appeal. 50 U.S.C. § 1806(h). In the unlikely event that the Court concludes that disclosure of any item within any of the FISA materials or suppression of any FISA-obtained or -derived information may be required, given the significant national security consequences that would result from such disclosure or suppression, the Government would expect to pursue an appeal. Accordingly, the Government respectfully requests that the Court indicate its intent to do so before issuing any order, and that the Court stay any such order pending an appeal by the United States of that order.

U.S. v. SAMI OSMAKAC

Case No. 8:12-CR-45-T-35AEP

CERTIFICATE OF SERVICE

I hereby certify that on June 14, 2013, I electronically filed the foregoing with the Clerk of Court by Using the CM/ECF system which will send a notice of electronic filing to the following:

George E. Tragos, Esq.

s/Sara C. Sweeney
Sara C. Sweeney
Assistant United States Attorney
United States Attorney No. 0000119
400 N. Tampa St., Suite 3200
Tampa, Florida 33602
Telephone (813) 274-6000
Facsimile (813) 274-6178
sara.sweeney@usdoj.gov

UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
TAMPA DIVISION

UNITED STATES OF AMERICA

Case No. 8:12-CR-45-T-35AEP

v.

DECLARATION AND CLAIM
OF PRIVILEGE

SAMI OSMAKAC

DECLARATION AND CLAIM OF PRIVILEGE
OF THE ATTORNEY GENERAL OF THE UNITED STATES

I, Eric H. Holder, Jr., hereby declare the following:

1. I am the Attorney General of the United States of America and head of the United States Department of Justice, an Executive Department of the United States. I have official custody of and control over the files and records of the United States Department of Justice. The matters stated herein are based on my knowledge, on consideration of information available to me in my official capacity as Attorney General, on discussions that I have had with other Department of Justice officials, and on conclusions I have reached after my review of this information.

2. Under the authority of 50 U.S.C. §§ 1806(f) and 1825(g), I submit this declaration pursuant to the Foreign Intelligence Surveillance Act of 1978 ("FISA"), as amended, in connection with the above-captioned criminal proceeding. I have been advised that the Government presently intends to use information obtained or derived from FISA-authorized electronic surveillance and physical searches in the criminal proceeding against the Defendant.

See 50 U.S.C. §§ 1806(c) and 1825(d). Accordingly, Defendant Sami Osmakac, by and through his attorney, has filed a motion seeking disclosure of FISA-related materials (hereinafter the “Defendant’s Motion”). The Government will file an opposition to the Defendant’s Motion. For the reasons set forth in the Government’s Opposition, it is necessary to provide this Court with the applications submitted to, and the orders issued by, the Foreign Intelligence Surveillance Court (“FISC”), and other related documents (hereinafter collectively referred to as “FISA Materials”).

3. Based on the facts and considerations set forth below, I hereby claim that it would harm the national security of the United States to disclose or to hold an adversarial hearing with respect to the FISA Materials. The United States will be submitting the relevant classified documents to this Court as part of a “Sealed Appendix,” so that this Court may conduct an *in camera, ex parte* review of the legality of the FISA collection at issue. My Claim of Privilege also extends to the classified portions of any memoranda and briefs the Government may file in connection with this litigation and to any oral representations that may be made by the Government that reference the classified information contained in the FISA Materials. In addition, should the defendant file a motion for suppression of evidence obtained or derived from FISA-authorized electronic surveillance and physical searches, my Claim of Privilege also extends to the classified portions of any memoranda the Government may file in connection with such litigation and to any oral representations that may be made by the Government that reference the classified information contained in the FISA Materials.

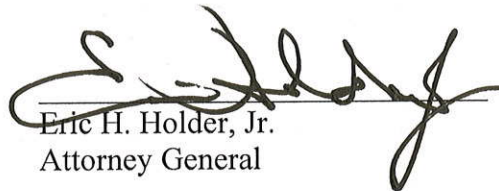
4. In support of my Claim of Privilege, the United States is submitting to the Court for *in camera, ex parte* review the Declaration of Andrew G. McCabe, Assistant Director, Counterterrorism Division, Federal Bureau of Investigation. Mr. McCabe’s Declaration sets

forth, in detail, the specific facts on which my Claim of Privilege is based. The Declaration of Mr. McCabe is classified at the "SECRET" level.

5. Relying on the facts set forth in Assistant Director McCabe's Declaration, I certify that the unauthorized disclosure of the FISA Materials that are classified at the "SECRET" level could reasonably be expected to cause serious damage to the national security of the United States. The FISA Materials contain sensitive and classified information concerning United States intelligence sources and methods and other information related to efforts of the United States to conduct counterterrorism investigations, including the manner and means by which those investigations are conducted. As a result, the unauthorized disclosure of that information could harm the national security interests of the United States.

6. I respectfully request that the Court treat the contents of the Sealed Appendix, for security purposes, in the same sensitive manner that the contents were treated in the submission to this Court, and to return the Sealed Appendix to the Department of Justice upon the disposition of the Defendant's Motion. The Department of Justice will retain the Sealed Appendix under the seal of the Court subject to any further orders of this Court or other courts of competent jurisdiction.

Pursuant to Title 28, United States Code, Section 1746, I declare under penalty of perjury that the foregoing is true and correct. Executed on June 11, 2013.


Eric H. Holder, Jr.
Attorney General